





2008-02-01

# Security Risks to the Oil and Gas Industry: Terrorist Capabilities by Friedrich Steinhausler, P. Furthner, W. Heidegger, S. Rydell, and L. Zaitseva; Strategic Insights, v. 7 issue 1 (February 2008)

# Security Risks to the Oil and Gas Industry: Terrorist Capabilities

## *Strategic Insights*, Volume VII, Issue 1 (February 2008)

by Friedrich Steinhäusler, P. Furthner, W. Heidegger, S. Rydell, and L. Zaitseva

*Strategic Insights* is a bi-monthly electronic journal produced by the Center for Contemporary Conflict at the Naval Postgraduate School in Monterey, California. The views expressed here are those of the author(s) and do not necessarily represent the views of NPS, the Department of Defense, or the U.S. Government.

## 1. Introduction: Current Terrorist Capabilities

Attacks on oil and gas installations have become the weapon of choice for international terrorism, irrespective of the political system and social-financial boundary conditions of the society under attack, for example: (a) In Columbia the terrorist groups FARC and ELN have attacked the national pipeline *Cano Limon-Covenas* so many times over the past five years that it has become known as *The Flute*;[1] (b) in 2004 Chechen terrorists have been able to blow up several pipelines in and around Moscow, Volgograd, Dagestan and Stavropol despite increased efforts by the Russian security forces;[2] (c) in 2006 the Indian terrorist group ULFA staged several pipeline attacks in the oil-rich region of Assam;[3] (d) repeated acts of pipeline sabotage in Iraq cost the country just in the first two years since the invasion in March 2003 more than US$10 billion in oil revenues;[4] (e) in Mexico six simultaneous attacks by EPR terrorists against oil and gas pipelines on September 10, 2007 caused severe supply shortages, leading to the temporary closure of several factories.[5] In the following sections current operational capabilities of terrorist are analyzed.

### *1.1 Terrorist Attack on Development and Exploration Sites*

Development and exploration sites are frequently located in remote areas, characterized by poor transport connections and communication to the authorities and the associated security infrastructure. If national security forces are supplied to guard the site, they are usually outnumbered by the attackers, who typically are members of the surrounding communities. Therefore these sites represent attractive targets for terrorists, e.g., in January 2006 gunmen using speedboats invaded the Benisede oil platform operated by SHELL in the Niger Delta.[6] Several soldiers guarding the flow station were killed in the attack; five workers were injured. In addition, two staff accommodation blocks were burnt down and processing facilities damaged during the attack.

### *1.2 Terrorist Attack during Maritime Transport*

Ships at sea are at risk of becoming targets for a terrorist attack for several reasons: (a) Security countermeasures on board are usually limited to high- pressure water hoses or high-powered sirens to ward off potential attackers; (b) The number of crew available for defense is rather low; (c) The load onboard represents a flammable and environmentally hazardous product; (d) External security support is only available with considerable time delay, if at all. Therefore tankers

are relatively easy targets for terrorist, as was demonstrated in October 2002 off the coast of Yemen. The supertanker *Limburg,* carrying 397,000 barrels of crude oil, was rammed by an explosive-laden dinghy on its starboard side. This attack resulted in one dead and twelve injured crew members. The Gulf of Aden suffered severe environmental damage due the uncontrolled spillage of 90,000 barrels of crude oil. The damage to the ship itself amounted to 30 million EURO.[7]

### *1.3 Terrorist Attack on the Distribution System*

Long-distance distribution of oil and gas is carried out by pipelines. These pipelines are built either above ground and therefore highly visible, or buried underground but frequently identifiable by markers placed above ground. In addition, auxiliary installations, such as compressor stations, are usually without any significant physical protection. The remoteness of the installations adds to their vulnerability from terror attacks. Under these circumstances it is not surprising that, for example, in the period June 12, 2003 to November 2, 2006, altogether 374 attacks have been carried out on national pipelines and associated installations in Iraq, i.e., almost ten attacks per month despite the major efforts by security forces to ensure their unimpeded operation.[8]

### *1.4 Terrorist Attack on a Refinery*

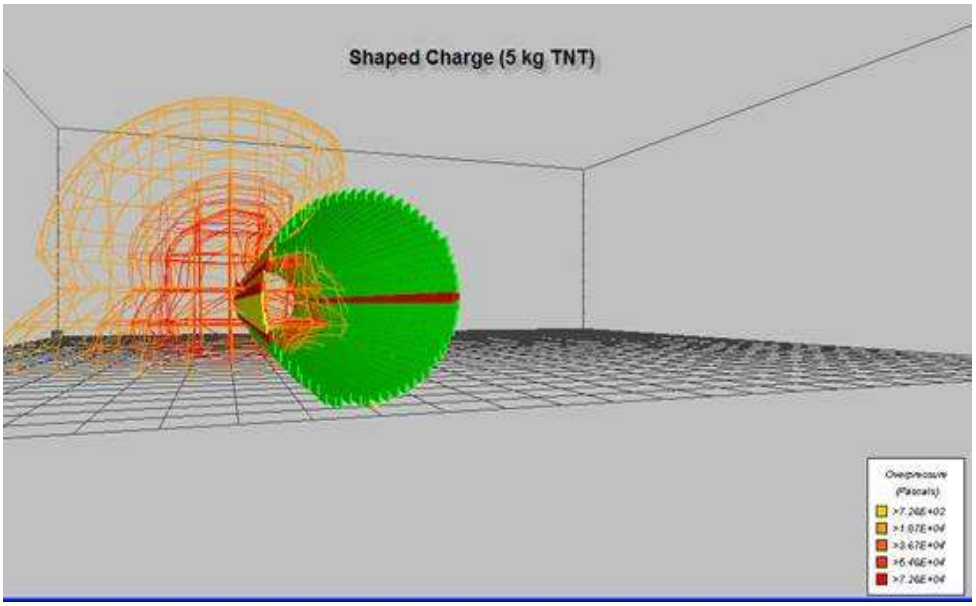
A refinery represents the most valuable asset in the oil and gas fuel cycle: only its continuous operation ensures the national energy security. In many countries the refining capacity is stretched to the limit, with little, if any, significant spare capacity. The large area covered by a refinery, its operational complexity, and the significant flow of people (staff and external subcontractors) and materials represent a major security challenge. This fact is usually acknowledged by facility management and national authorities by providing several layers of security around such a facility. The value of such increased security measures was clearly demonstrated in the foiled terrorist attack on the world's largest refinery in Abqaiq (Saudi Arabia) on February 24, 2006.[9] Terrorists in two explosives-laden vehicles were able to penetrate the first ring of security, wearing fake uniforms and driving in cars with Saudi oil company logos. However, they failed to penetrate the second ring of security and had to engage in an extended battle with the security forces. The foiled attack resulted in two dead attackers and two wounded guards but the refinery itself remained undamaged without interruption of its operation.

## 2. Future Potential Security Threats to the Oil- and Gas Fuel Cycle

### *2.1 Coordinated Terrorist Attacks on Multiple Development and Exploration Sites*

Oil or gas exploration occurs usually in fields encompassing many individual exploration sites, stretching over large distances in remote areas. It is difficult to prevent intrusion from the outside, since attackers can use speed-boats (e.g., Nigeria), 4WD vehicles (e.g., Saudi Arabia), or unmanned aerial vehicles (UAV).[10] Consequently terrorists can carry out coordinated attacks on individual oil and gas exploration sites within the field. The amount of explosives required for such an attack is relatively small (e.g., it has been shown that 5 kg of TNT for a single site is sufficient), enabling one individual to carry several such devices at once. Figure 1 shows the destruction of a pipeline resulting from the detonation of a shaped charge: the pipeline is totally destroyed (red and yellow contours). Since shaped charges are commonly used in oil fields, they become readily available weapons for terrorists and are found in the vicinity of the target.[11]

**Figure 1: Structural damage (overpressure iso-curves) resulting from the detonation of a shaped charge (5 kg TNT) attached to a pipeline section**




A coordinated attack scenario on an exploration site could contain the following components: (a) Kidnapping of employees; (b) Suicide truck bomb/car bomb convoy against drilling installations; (c) Covert attack against auxiliary buildings; (d) Attack on the communication system. The logistical requirements are summarized in Table 1.

**Table 1: Logistical requirements for a coordinated attack on multiple oil-/gas exploration sites**

| Terrorist Action | Logistical Requirements |
|---|---|
| Kidnapping/murder of employees | • >5 armed terrorist<br>• 4WD vehicle<br>• Apartment as hide-out |
| 1. Suicide truck bomb/car bomb convoy against drilling station | • >2 terrorists<br>• Truck<br>• 4WD vehicle<br>• 2,500 kg ANFO |
| 2. Cover attack on auxiliary buildings | • >10 armed terrorists<br>• >3 4WD vehicles |
| 3. Destruction of pipeline and compressor stations | • >2 terrorists<br>• 4WD vehicle<br>• Shaped charges |
| 4. Attack on the communication system | • 1 terrorist (*hacker*) |

The information and communication system used during oil exploration and development phase is of vital importance for the success of such an operation. In terms of security this phase represents multiple challenges:

1. Large number of staff operating at the site;
2. Large number of contractors entering and leaving the site;
3. High volume of sensitive alphanumerical information transmitted from the field operation to headquarters or regional offices and back.

For economic and competitive reasons all of these operations occur under high time pressure, i.e., the potential for lax security or errors in implementing security procedures is significant. These valuable data are subject to the following security risks: tampering with technical data; theft of strategic data; intrusion into a valuable company database; undetected hacking into the system; data snooping; introducing malware into the system. The additional possibility of insider support would enhance the damage potential significantly.

The impact of a similar, but significantly simpler attack scenario could be seen at the end of the 1990-1991 Gulf War in Kuwait, where more than 700 oil wells were intentionally set on fire by the retreating Iraqi forces in 1991.[12] The associated clean-up costs were estimated at more than US$ 700 million.[13]

### *2.2 Suicide Terrorist Attack of an Offshore Platform*

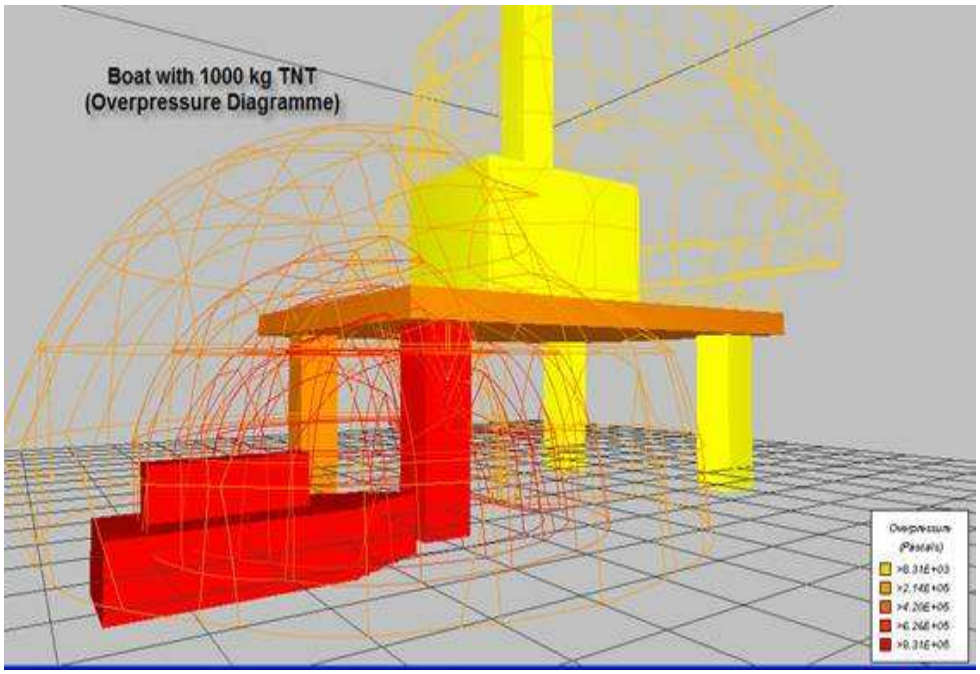
Offshore platforms are subject to increased physical protection as part of the national framework of critical infrastructure, i.e., the airspace and the approach by sea is subject to continuous surveillance and optional military intervention. However, as the terrorist attack on the *USS Cole* in Yemen in 2000 demonstrated, even a battle ship with its enhanced technical and operational capabilities to ward off an enemy attack has proven to be vulnerable to a suicide terrorist boat attack. Table 2 summarizes threat scenarios and the associated logistical requirements for terrorists to stage a successful attack against an offshore platform.

**Table 2: Logistical requirements for a suicide terrorist attack against an offshore platform**

| Terrorist Action | Logistical Requirements |
|---|---|
| 1. Suicide attack with light general aviation (GA) aircraft with explosives onboard | • 2 pilot terrorists<br>• >400 kg of explosives<br>• Chartered/diverted GA aircraft |
| 2. Suicide attack with three high speed boats with explosives onboard | • 3 chartered high speed boats<br>• 3 pilot terrorists<br>• >1,000 kg explosives in each boat |
| 3. Covert underwater attack with divers and explosives | • 5 specially trained terrorists<br>• 100 kg explosives (shaped charges)<br>• Mini-submarine or suicide torpedo[17] |

Figure 2 shows the damage to an offshore platform due to the attack with a boat detonating 1,000 kg TNT upon impact at one of the columns carrying the structure. The platform suffers extensive structural damage (red and yellow overpressure iso-curves), rendering it inoperable.

**Figure 2: Structural damage (overpressure iso-curves) to an offshore platform resulting from a suicide boat attack with 1,000 kg TNT onboard**




### *2.3 Coordinated Terrorist Attacks Against the Distribution and Retailing Sector*

The distribution of the products from the refinery to the retailing sector is basically an open system in which the most vulnerable component, i.e., the truck or railcar, is clearly marked as carrying hazardous, flammable products. Every gasoline-truck or propane-loaded railcar is highly visible in the flow of traffic. Both modes of transport have periods where vehicles are stationary (during loading/unloading or parking), i.e., facilitating an attack as compared to a moving target. Also the endpoint, the location where the actual sale of the product occurs, is generally without any significant physical security (e.g., filling station; storage area for propane bottles). Frequently these sites are located in areas with high population density, thereby increasing the number of victims in view of the explosive potential of the fuel and gas. Concurrent environmental damage resulting from an uncontrolled release may be seen as an “added value” by terrorists. Table 3 lists the security risks to the distribution- and retail sector and the associated logistical requirements for terrorists.

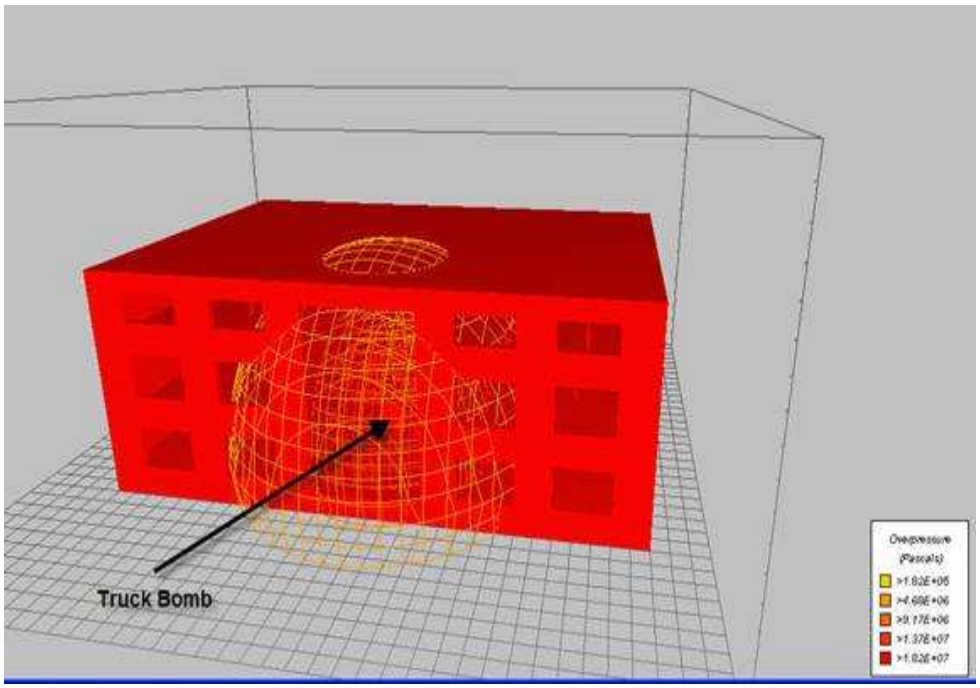
It can be safely stated that international terrorist groups are able to fulfill the logistical requirements to carry out successful attacks on any component of the distribution and retail sector of the oil and gas industry. Although the damage potential for each retail site is limited, a coordinated attack on several such sites represents a significant disruption of the national economy with major socio-political implications. For example, it is feasible to consider a chain of terror attacks on filling stations across a nation with relatively low probability for the security forces being able to interdict such attacks in view of the large number of such sites in any given country. In addition to the ease of implementing such acts of terror, attacks on filling stations are attractive for terrorists because of the ensured media attention.

Also the misuse of a gasoline filled tanker truck as a weapon by driving it into a building requires relatively little operational skills by the terrorists. In Figure 3 the destruction of an office building by a detonating tanker truck is shown. The energy release during the explosion—even disregarding the subsequent fire damage—is sufficient to largely destroy the building.

**Table 3: Logistical requirements for terrorist attacks on the distribution- and retail sector of the oil and gas industry**

| Terrorist Action | Logistical requirements |
|---|---|
| 1. Hijacking of a fuel truck and use as a weapon | • >2 armed terrorists<br>• Vehicle |
| 2. Contamination of fuel with chemicals (e.g. Na, P) to ignite the cargo | • 1 terrorist<br>• Chemicals |
| 3. Attack on a stationary fuel truck at a filling station | • 1 terrorist<br>• Explosives |
| 4. Covert placement of an explosive/incendiary device on a railcar or fuel truck. Activation via remote control when truck reaches sensitive area (Aircraft, dense populated areas) | • 1 terrorist<br>• Explosives/chemicals |
| 5. Attack on stationary railcars at depot | • >2 terrorists<br>• Vehicle<br>• Rocket-propelled grenades (RPG) |

**Figure 3: Structural damage (overpressure iso-curves) to a multi-storey office building due to the detonation of a suicide truck bomb (8,000 kg TNT)**



## 3. Conclusions

Every sector of the oil and gas fuel cycle is vulnerable to terrorist threats to a varying degree. Neither intelligence services, nor military forces have been able to prevent terror attacks from happening. However, several terror attacks on oil and gas installations have been foiled by well trained- and equipped security forces, e.g., in Saudi Arabia.

International terrorism is very well aware of the critical and vital aspects of a secure energy supply to industrialized nations worldwide and has demonstrated its ability to stage successful attacks on exploration sites, pipeline systems, refineries and the distribution of the final products, in the retail sector. An analysis of the logistical requirements for ten likely attack scenarios described in Tables 1, 2 and 3 shows that most of them are within the realm of international terrorism groups. Some of the technical and operational challenges have already been overcome by organized crime networks (e.g., drug traffickers) or advanced national terrorist organizations against national Armed Forces (e.g., Tamil Tigers). Therefore it is only a question of when, but not if, the attack scenarios outlined here will actually be deployed against the oil and gas industry on a global scale. The probability of success ranges from *low* in the case of an attack on an offshore oil/gas platform to *high* for coordinated multiple attacks on gasoline filling stations.

Over the next twenty five years oil and gas will provide about 60 percent of global energy and therefore remain the prime source of energy for industrialized and developing countries alike. In view of the attractiveness of the oil and gas industry as a major component of every national critical infrastructure, high success rates in terror attacks on some components of this industry hitherto and the relatively low logistical requirements for even more sophisticated threat scenarios, the probability for an increased number of terror attacks and a higher level of their sophistication will increase. The U.S. National Intelligence Estimate states in 2007 that: (a) al-Qaeda has been able to re-organize despite of worldwide persecution and U.S. attacks; (b) al-Qaeda has set up the most stable training program since 2001.[14] Therefore, al-Qaeda and its network are likely to increase their activities in order to disrupt the oil- an gas fuel cycle worldwide. On a global scale, areas with major security problems in the near term are located in the Middle East, Africa, Central Asia, and Asia:

### *The Middle East:*

The Middle East holds between two-thirds and three-quarters of all known oil reserves.[15] In 2004 four of the top five nations with the greatest known oil reserves were Arab nations, with oil reserves totaling 613 billion barrels. This politically volatile region is also home to the world's largest oil processing plant *Abqaiq* with a capacity of up to 6.8 million barrels/day. A successful terror attack disrupting operations for an extended period would have global repercussions. Another region at major risk is the *Strait of Hormuz,* representing a potential bottleneck for oil supplies. Every day up to 17 million barrels of oil (equal to 20 percent of the global oil supply) pass through two channels, each about 1.5 km wide. To a lesser extent also the *Suez Canal* falls into this category, where about 1.3 million barrels/day pass through a shipping lane with a width of about 350 m. A successful terror attack on tankers, e.g., with anti-ship missiles, could result in one or more ships blocking the passage and thereby interrupting global supplies.

### *Africa:*

In *Algeria* national terrorist activities as part of the ongoing civil war have resulted in 150,000 to 200,000 deaths between 1991 and 2002. The probability increases that future activities (*Armed Islamic Group*, GIA) will involve also oil and gas installations. In *Niger* the local Movement for the Emancipation of the Niger Delta, backed by large segments of the population, is likely to continue

its repeated attacks on oil and gas installations in the exploration area of the Delta in the form of pipeline rupture, kidnappings and sabotaging oil fields.

### *Central Asia:*

The *Baku-Tbilisi-Ceyhan pipeline* is at risk from regional insurgents and members of al-Qaeda who are reportedly planning acts of sabotage.[16] The *Kazakhstan-Xinjiang pipeline* is facing increasing terror attacks by hostile Muslim Uighur minorities. The *Southeast Turkey pipeline* is threatened by a bomb attack campaign carried out by guerrillas belonging to the Kurdistan Workers Party (PKK). The *Druzhba pipeline,* extending over 4,000 km, is the longest pipeline in the world, has a capacity of 1.2 million barrels/day. Its route runs through areas of high political volatility in the North-Caucasus region of Russia. In view of its strategic importance for the energy supply of Ukraine and Germany, this pipeline represents a high value target for terrorists.

### *Asia:*

The 130 ships, including tankers, passing through the *Strait of Malacca* every day represent 20 percent of the world trade. If this narrow passage should be blocked by a terrorist attack on one or more ships (e.g., deployment of naval mine), trade in general and the energy supply in particular for major industrial countries in the region would be severely threatened. Since the area is suffering severe security threats due to piracy already, it can no longer be assumed that in the future terrorists will not join forces with other criminal elements operating successfully in the Straits.

## 4. Recommendations

In order to counter the increasing security threat to the oil and gas industry worldwide it is recommended to engage in a proactive global two-pronged initiative, combining aspects of security strategy and operational security.

### *4.1 Security Strategy*

Terrorists are likely to deploy increasingly sophisticated modes of attack, including: (a) Synchronized attacks on several components of the oil and gas fuel cycle; (b) Hostile acts against security forces responding to the emergency. Therefore security of the oil and gas fuel cycle, from the front end of exploration to the back end of supply and distribution, will have to be considered a national strategic issue. A possible way forward could be the application of the *Concept of Integrated Physical Protection*, consisting of:

1. State-of-the-art technical and operational countermeasures, enabling the management to reduce the probability of success of a terror attack;

2. Increased emphasis on Corporate Security Culture, thereby strengthening corporate resilience to the consequences of a terror attack and minimizing the insider threat;

3. Continuous Security Training at all levels in order to reduce the probability for a terror attack to happen and to reduce downtime after a terror attack;

4. Regular Threat and Risk assessment in order to identify, qualify and quantify risks and countermeasures in a changing environment;

5. Evaluation and update of strategies and countermeasures based on risk analyses by considering the cost benefit factor;

6. Strengthen the cooperation with related government security agencies and first responders.

### *4.2 Operational Security*

Major efforts are currently underway to strengthen assessment and countermeasure capabilities and thereby minimize security risks:

a) *Technological Developments*: Integrated 3D-Vulnerability Assessment using advanced geographical information systems and combining satellite monitoring data with ground-based data sets; Real-time information using seismic sensing alarms for instant notification of rapid-response teams; Deployment of UAV equipped with automatic weapons; Unmanned helicopters capable of image processing; Fortification of pipelines with external carbon fibre wrap.

b) *Logistics:* Shortening lead time between attack and repair; Maintaining adequate inventory of custom-made spare parts; Strengthening physical protection at critical junctions, based on 3D-vulnerability analysis; Enhanced physical access control (e.g., intelligent smart card-based systems); Secure data communication (e.g., encryption); Progressively restricted access areas upon approaching high value target areas (*Onion skin principle*); Enhanced GPS-3 or Galileo-based positioning devices for vehicle fleet; Real-time vehicle data monitoring (vehicle movement data; vehicle tampering alert; open voice communications between dispatchers, drivers and customers).

c) *Training and Policy:* Implementation of Industrial corporate security awareness programs (*ICSAP*) to develop a security culture and policy. Security training for all personnel, security strategies for human resource management and administration. Insider identification strategies and cooperation with First responder (drills and training). Contingency planning, crisis and disaster management on all levels. Global communication and marketing of security as a preventive tool. Social and humanitarian support programs as preventive tools.

## About the Author

Friedrich Steinhäusler is Full Professor of Physics and Biophysics at the University of Salzburg and Director of the Salzburg Government Radiological Measurements Laboratory. His main fields of research activity are nuclear security and safety, terrorism and emergency preparedness. In July 2005, he organized the international conference “NUSEC-Nuclear Energy and Security,” the first in a series of conferences dedicated to the security of various energy sectors conducted at the University of Salzburg. Subsequently he organized “PETROSEC&SEIF-CV: Petroleum Supply Chain and Security” in 2007. In the recent past he was Director of the NATO CLG Expert Group "Terrorism Threats against Nuclear Power Plants and Spent Fuel Transport," Co-Director of the NATO ARW "Catastrophic Terrorism and First Responders," Co-Director of the NATO STS-CNAD “Emergency Management after a Major Terror Attack,” and Chairman of the US-German ERP Expert Group "Global Fight Against Terrorism." From 1999 to 2003 he served as Program Manager for *Security & Technology* at the European Forum (Stanford University, California, USA) ) and from 2001 to 2003 as Project Manager for "Protection of Nuclear Material Against Theft and Sabotage" at Stanford University’s Center for International Security and Cooperation.

## References


1. “Oil, Terrorism and Drugs Intermingle in Colombia,” *IAGS Energy Security Brief*, August 5, 2003.

2. Roman Kupchinsky, “Chechnya: Stolen Oil and Purchased Guns,” *Radio Free Europe/Radio Liberty*, October 25, 2005.

3. “Pipeline Sabotage Is Terrorist’s Weapon of Choice,” *IAGS Energy Security Brief*, March 28, 2005.

4. Gal Luft, “Pipeline Sabotage is Terrorist’s Weapon of Choice,” *IAGS Pipeline & Gas Journal*, March 28, 2005.

5. Miguel Hernandez, “Mexican Rebels Claim Pipeline Attacks,” *Associated Press*, September 11, 2007.

6. “Speedboat Attack on Nigeria Rig,” *BBC News*, January 16, 2006.

7. Wikipedia, "Maritime Jewel," *Wikipedia.org*, the free encyclopedia.

8. "Iraq Pipeline Watch," *IAGS Energy Security*.

9. “Bombers Attempt Attack on Saudi Oil Facility,” *International Herald Tribune*, February 24, 2006.

10. Current pilot-less drones (wingspan: 5m; payload: 50 kg) are equipped with GPS and undetectable by radar, causing concern for the security community. "We’re observing an increasing threat from such thing as remote-controlled aircraft used as small flying bombs against soft targets." Michael Gauthier, Head, Secret Service, Calgary, Alberta, as quoted in "Flying Robot Attack 'Unstoppable': experts," *Breitbart.com*, May 9, 2006.

11. Wikipedia, "Shaped Charge," *Wikipedia.org*, the free encyclopedia.

12. T. Husain, *Kuwaiti Oil Fires: Regional Environmental Perspectives* (Amsterdam: Elsevier/Pergamon, 1995).

13. “UK: Iraq torches seven oil wells,” *CNN*, March 21, 2003.

14. See Table 2. "National Intelligence Estimate: The Terrorist Threat to the U.S. Homeland," *GlobalSecurity.org*, July 2007.

15. Shibley Telhami, "The Persian Gulf: Understanding the American Oil Strategy," *The Brookings Review*, Spring 2002, Vol. 20, No. 2, pp.32-35.

16. Namiq Abbasov, Minister of National Security, Azerbaijan, 2005.

17. A miniature submarine has already been built by South American drug-traffickers; suicide torpedoes have been deployed by Tamil Tiger against the Navy in Sri Lanka.